CIS Benchmarks

CIS Google Chrome Benchmark

v1.3.0 - 08-15-2018

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Terms of Use 1
Overview 4
Intended Audience 4
Consensus Guidance 4
Typographical Conventions 5
Scoring Information 5
Profile Definitions 6
Acknowledgements 7
Recommendations 8
1 Computer Configuration 8
1.1 Google Chrome 8
1.1.1.1 (L1) Ensure 'Configure the required domain names for remote access hosts' is set to 'Enabled' (Scored) 8
1.1.1.2 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled' (Scored) 10
1.1.1.3 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored) 12
1.1.1.4 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Scored) 14
1.1.2.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session) (Scored) 16
1.1.2.2 (L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play) (Scored) 18
1.1.4.1 (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions) (Scored) 20
1.1.8.1 (L1) Ensure `Configure native messaging blacklist` is set to 'Enabled' ("*" for all messaging applications) (Scored) 22
1.1.10.1 (L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Scored) 24
1.1.11.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) (Scored) 26

1.1.15 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled' (Scored) 28
1.1.16 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored) 30
1.1.17 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored) 32
1.1.18 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored) 34
1.1.19 (L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored) 36
1.1.20 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored) . 38
1.1.21 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored) 40
1.1.22 (L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Scored) 42
1.1.23 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored) 44
1.1.24 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored) 46
Appendix: Summary Table 48
Appendix: Change History 50

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Google Chrome Browser. This guide was tested against Google Chrome v68.0.3440.75. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Google Chrome.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Editor
Brian Howson

Recommendations

1 Computer Configuration

The following structure of this guide mirrors how it is structured in the Google Chrome Group Policy template.

1.1 Google Chrome

This section contains recommendations for Google Chrome.

1.1.1 Configure Remote Access Options

This section contains recommendations for Configuring Remote Access Options

1.1.1.1 (L1) Ensure 'Configure the required domain names for remote access hosts' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows the user to configure a required host domain that is imposed on remote access hosts. When enabled, hosts can only be shared using accounts that are registered to the specified domain.

Rationale:

If this setting is disabled or not set, then hosts can be shared using any account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\RemoteAccessHostDomainList
:1
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` and enter domain.

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Configure remote access options\Configure the required domain names
for remote access hosts
```

Impact:

If this setting is enabled, hosts can be shared only using accounts registered on the specified domain name.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostClientDomain

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

1.1.1.2 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows the user to disable a remote user's physical input and output while the remote connection is in progress.

Rationale:

If this setting is disabled or not set, then both local and remote users can interact with the host when it is being shared.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostRequireCur
tain
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Configure remote access options\Enable curtaining of remote access
hosts
```

Impact:

If this setting is enabled, host's physical input and output devices are disabled while a remote connection is in progress.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostRequireCurtain

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

1.1.1.3 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome enables the usage of STUN servers which allows remote clients to discover and connect to a machine even if they are separated by a firewall. By disabling this feature, in conjunction with filtering outgoing UDP connections, the machine will only allow connections from machines within the local network.

Rationale:

If this setting is enabled, remote clients can discover and connect to this machines even if they are separated by a firewall.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostFirewallTraversal
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
 Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Enable firewall traversal from remote access host
```

Impact:

If this setting is disabled and outgoing UDP connections are filtered by the firewall, this machine will only allow connections from client machines within the local network.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostFirewallTraversal

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

1.1.1.4 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome enables a user to opt-out of using user-specified PIN authentication and instead pair clients and hosts during connection time.

Rationale:

If this setting is enabled or not configured, users can opt to pair clients and hosts at connection time, eliminating the need to enter a PIN every time.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowClientPairing
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Enable or disable PIN-less authentication
```

Impact:

If this setting is disabled, users will be required to enter PIN every time.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostAllowClientPairing

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

1.1.2 Content Settings

This section contains recommendations for Content Settings

1.1.2.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session) (Scored)

Profile Applicability:

- Level 2

Description:

Allows you to set whether websites are allowed to set local data. Setting local data can be either allowed for all websites or denied for all websites.

Rationale:

If this policy is left not set, `AllowCookies` will be used and the user will be able to change it.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultCookiesSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
Settings\Default cookies setting
```

Impact:

If this setting is enabled, cookies will be cleared when the session closes.

Default Value:

If this policy is left not set, `AllowCookies` will be used and the user will be able to change it.

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultCookiesSetting

CIS Controls:

Version 6

13 Data Protection
Data Protection

1.1.2.2 (L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play) (Scored)

Profile Applicability:

- Level 1

Description:

Allows you to set whether websites are allowed to automatically run plugins. Automatically running plugins can be either allowed for all websites or denied for all websites.

Rationale:

Malicious plugins can cause browser instability and erratic behavior so setting the value to click to play will allow a user to only run necessary plugins.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultPluginsSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with click to play selected from the drop down.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
Settings\Default Flash Setting
```

Impact:

If this setting is enabled, users must click plugins to allow their execution

Default Value:

If this policy is left not set, the user will be able to change this setting manually.

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultPluginsSetting

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

1.1.3 Default Search Provider

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.4 Extensions

This section contains recommendations for Extensions

1.1.4.1 (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions) (Scored)

Profile Applicability:

- Level 1

Description:

Enabling this setting allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blacklisted.

Rationale:

This can be used to block extensions that could potentially allow remote control of the system through the browser. If there are extensions needed for securing the browser or for enterprise use these can be enabled by configuring the extension whitelist.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallBlacklist:
1
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Extensions\Configure Extension Installation Blacklist
```

Impact:

Any installed extension will be removed unless it is specified on the extension whitelist.

Default Value:

If this policy is left not set the user can install any extension in Google Chrome.

References:

1. https://www.chromium.org/administrators/policy-list-3#ExtensionInstallBlacklist

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

1.1.5 Google Cast

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.6 Home Page

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.7 Locally Managed Users Settings

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.8 Native Messaging

This section contains settings for Native Messaging.

1.1.8.1 (L1) Ensure `Configure native messaging blacklist` is set to 'Enabled' ("" for all messaging applications) (Scored)*

Profile Applicability:

- Level 1

Description:

Allows you to specify which native messaging hosts that should not be loaded.

NOTE: A blacklist value of '*' means all native messaging hosts are blacklisted unless they are explicitly listed in the whitelist.

Rationale:

For consistency with Plugin and Extension policies, native messaging should be blacklisted by default, requiring explicit administrative approval of applications for whitelisting. Examples of applications that use native messaging is the 1Password password manager.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\NativeMessagingBlacklist:1
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Native Messaging\Configure native messaging blacklist
```

Impact:

A blacklist value of '*' means all native messaging hosts are blacklisted unless they are explicitly listed in the whitelist.

Default Value:

If this policy is left not set Google Chrome will load all installed native messaging hosts.

References:

1. https://www.chromium.org/administrators/policy-list-3#NativeMessagingBlacklist

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

1.1.9 New Tab Page

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.10 Password Manager

This section contains recommendations for Password Manager

1.1.10.1 (L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome will memorize passwords and automatically provide them when a user logs into a site. By disabling this feature the user will be prompted to enter their password each time they visit a website.

Rationale:

If this setting is enabled, users can have Google Chrome memorize passwords and provide them automatically the next time they log in to a site. An intruder who has unrestricted access to your computer for even a minute can view and copy all of your saved passwords just by visiting an easy-to-remember settings page: chrome://settings/passwords.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PasswordManagerEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Password manager\Enable the password manager
```

Impact:

If this settings is disabled, users cannot save new passwords but they may still use passwords that have been saved previously.

Default Value:

Not Configured.

References:

1. https://www.chromium.org/administrators/policy-list-3#PasswordManagerEnabled

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

1.1.11 Policies for HTTP Authentication

This section contains Policies for HTTP Authentication.

1.1.11.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) (Scored)

Profile Applicability:

- Level 1

Description:

Specifies which HTTP authentication schemes are supported by Google Chrome.

Rationale:

Possible values are 'basic', 'digest', 'ntlm' and 'negotiate'. Basic and Digest authentication do not provide sufficient security and can lead to submission of users password in plaintext or minimal protection.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AuthSchemes
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled:(ntlm, negotiate)`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Policies
for HTTP Authentication\Supported authentication schemes
```

Default Value:

Not configured (all four schemes will be used)

References:

1. https://www.chromium.org/administrators/policy-list-3#AuthSchemes

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

1.1.12 Proxy Server

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.13 Safe Browsing settings

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.14 Startup Pages

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.1.15 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 2

Description:

Allows access to local files on the machine by allowing Google Chrome to display file selection dialogs.

Rationale:

Preventing users from uploading documents can help limit the loss of sensitive information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowFileSelectionDialogs
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow invocation of file selection dialogs
```

Impact:

If you enable this setting, users can open file selection dialogs as normal.

Default Value:

If this setting is not set, users can open file selection dialogs as normal.

References:

1. https://www.chromium.org/administrators/policy-list-3#AllowFileSelectionDialogs

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

1.1.16 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome enables the use of outdated plugins. By disabling this feature Chrome will not prompt the user to use an outdated plugin.

Rationale:

Running the most up-to-date version of a plugin can reduce the possibility of running a plugin that contains an exploit or security hole.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowOutdatedPlugins
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow
running plugins that are outdated
```

Impact:

If you disable this setting, outdated plugins will not be used and users will not be asked for permission to run them.

Default Value:

If this setting is not set, users will be asked for permission to run outdated plugins.

CIS Controls:

Version 6

7.1 Use Only Fully-supported Web Browsers And Email Clients
Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.

1.1.17 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows cookies to be set by web page elements that are not from the domain in the user's address bar. Enabling this feature prevents third party cookies from being set.

NOTE: Third Party Cookies and Tracking Protection are required for many business critical websites, including SalesForce and Office365.

Rationale:

Blocking third party cookies can help protect a user's privacy by eliminating a number of website tracking cookies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BlockThirdPartyCookies
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Block
third party cookies
```

Impact:

Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browser's address bar.

Default Value:

If this policy is left not set, third party cookies will be enabled but the user will be able to change that.

References:

1. https://www.chromium.org/administrators/policy-list-3#BlockThirdPartyCookies
2. https://help.salesforce.com/articleView?id=getstart_browser_recommendations.htm&type=5

CIS Controls:

Version 6

13 Data Protection
Data Protection

1.1.18 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows for processes started while the browser is open to remain running once the browser has been closed. It also allows for background apps and the current browsing session to remain active after the browser has been closed. Disabling this feature will stop all processes and background applications when the browser window is closed.

Rationale:

If this setting is enabled, vulnerable or malicious plugins, apps and processes can continue running even after Chrome has closed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BackgroundModeEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Continue
running background apps when Google Chrome is closed
```

Impact:

If this policy is set to Disabled, background mode is disabled and cannot be controlled by the user in the browser settings.

Default Value:

If this policy is left unset, background mode is initially disabled and can be controlled by the user in the browser settings.

References:

1. https://www.chromium.org/administrators/policy-list-3#BackgroundModeEnabled

CIS Controls:

Version 6

7 Email and Web Browser Protections
Email and Web Browser Protections

1.1.19 (L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows users to auto-complete web forms with saved information such as address, phone number and credit card numbers. Disabling this feature will prompt a user to enter all information manually.

Rationale:

If an attacker gains access to a user's machine where the user has stored auto save data, information could be harvested or used to gain access to more systems.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AutoFillEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
AutoFill
```

Impact:

If this setting is disabled, AutoFill will be inaccessible to users.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#AutoFillEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

1.1.20 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This setting enables Google Chrome to act as a proxy between Google Cloud Print and legacy printers connected to the machine.

Rationale:

Disabling this option will prevent users from printing possible confidential enterprise documents through the cloud.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintProxyEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Google Cloud Print Proxy
```

Impact:

If this setting is disabled, users cannot enable the proxy, and the machine will not be allowed to share its local printers with Google Cloud Print.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CloudPrintProxyEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

1.1.21 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This Setting controls anonymous reporting of usage and crash-related data about Google Chrome to Google.

NOTE: This policy is not available on Windows instances that are not joined to a Microsoft® Active Directory® domain.

Rationale:

Anonymous crash/usage data can be used to identify people, companies and information, which can be considered data ex-filtration from company systems.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:MetricsReportingEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
reporting of usage and crash-related data
```

Impact:

If this setting is disabled, this information is not sent to Google.

Default Value:

Not Configured

References:

1. https://www.chromium.org/administrators/policy-list-3#MetricsReportingEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

1.1.22 (L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy controls is every website will load into its own process.

Rationale:

Chrome will load each website in its own process. So, even if a site bypasses the same-origin policy, the extra security will help stop the site from stealing your data from another website.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SitePerProcess
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
Site Isolation for every site
```

Impact:

If the policy is enabled, each site will run in its own process which will cause the system to use more memory.

Default Value:

If the policy is not configured, the user will be able to change this setting.

References:

1. https://www.chromium.org/Home/chromium-security/site-isolation

CIS Controls:

Version 6

2.4 Use Of Virtual Machines For Risk Management

Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

1.1.23 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This setting enables Google Chrome to submit documents to Google Cloud Print for printing.

NOTE: This only affects Google Cloud Print support in Google Chrome. It does not prevent users from submitting print jobs on web sites.

Rationale:

Disabling this option will prevent users from printing possible confidential enterprise documents through the cloud.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintSubmitEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
submission of documents to Google Cloud print
```

Impact:

If this setting is disabled, users cannot print to Google Cloud Print from the Chrome print dialog

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CloudPrintSubmitEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

1.1.24 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls if saved passwords from the default browser can be imported.

Rationale:

In Chrome, passwords can be stored in plain-text and revealed by clicking the “show” button next to the password field by going to chrome://settings/passwords/.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportSavedPasswords
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Import saved passwords from default browser on first run
```

Impact:

If this setting is disabled, saved passwords from other browsers are not imported.

Default Value:

If it is not set, the user may be asked whether to import, or importing may happen automatically.

References:

1. https://www.chromium.org/administrators/policy-list-3#ImportSavedPasswords

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Computer Configuration**		
1.1	**Google Chrome**		
1.1.1	**Configure Remote Access Options**		
1.1.1.1	(L1) Ensure 'Configure the required domain names for remote access hosts' is set to 'Enabled' (Scored)	☐	☐
1.1.1.2	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled' (Scored)	☐	☐
1.1.1.3	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored)	☐	☐
1.1.1.4	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Scored)	☐	☐
1.1.2	**Content Settings**		
1.1.2.1	(L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session) (Scored)	☐	☐
1.1.2.2	(L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play) (Scored)	☐	☐
1.1.3	**Default Search Provider**		
1.1.4	**Extensions**		
1.1.4.1	(L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions) (Scored)	☐	☐
1.1.5	**Google Cast**		
1.1.6	**Home Page**		
1.1.7	**Locally Managed Users Settings**		
1.1.8	**Native Messaging**		
1.1.8.1	(L1) Ensure `Configure native messaging blacklist` is set to 'Enabled' ("*" for all messaging applications) (Scored)	☐	☐
1.1.9	**New Tab Page**		
1.1.10	**Password Manager**		
1.1.10.1	(L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Scored)	☐	☐
1.1.11	**Policies for HTTP Authentication**		
1.1.11.1	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) (Scored)	☐	☐
1.1.12	**Proxy Server**		
1.1.13	**Safe Browsing settings**		
1.1.14	**Startup Pages**		
1.1.15	(L2) Ensure 'Allow invocation of file selection dialogs' is set to	☐	☐

	'Enabled' (Scored)		
1.1.16	(L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)	☐	☐
1.1.17	(L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored)	☐	☐
1.1.18	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored)	☐	☐
1.1.19	(L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored)	☐	☐
1.1.20	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)	☐	☐
1.1.21	(L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored)	☐	☐
1.1.22	(L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Scored)	☐	☐
1.1.23	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored)	☐	☐
1.1.24	(L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
10-30-15	1.0.0	Initial Release
3-15-16	1.1.0	text to update on benchmarks_rule_1.11.1_Set_Enable_the_password_manager_to_Disabled
3-15-16	1.1.0	Removed version from Title
3-15-16	1.1.0	Updated all recommendation titles to include level and new wording.
6-28-17	1.2.0	Added Controls Mappings to all recommendations
6-28-17	1.2.0	Set 'Allow invocation of file selection dialogs' to Enabled - description / rationale error – Ticket #5105
6-28-17	1.2.0	Remove - (L1) Ensure 'Allow users to show passwords in Password Manager' is set to 'Disabled' – Deprecated – Ticket #4767
6-28-17	1.2.0	Remove - (L1) Ensure 'Specify a list of Disabled Plugins' is set to 'Enabled' - Deprecated – Ticket #4764
6-28-17	1.2.0	Remove - Set 'Enable alternate error pages' to Disabled – Ticket #5106
8-15-18	1.3.0	UPDATE - Policy name/audit consistency – Ticket #6519
8-15-18	1.3.0	REMOVE- deprecated plugin sections – Ticket #6073
8-15-18	1.3.0	UPDATE - Policy is renamed to "Default Flash setting" – Ticket #6520
8-15-18	1.3.0	UPDATE - RemoteAccessHostClientDomain deprecated – Ticket #5519
8-15-18	1.3.0	UPDATE - 1.3.2 (L1) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled' -- Unclear Guidance – Ticket #4765
8-15-18	1.3.0	UPDATE – Created new platform file to work on more installations. – Ticket #6249

8-15-18	1.3.0	UPDATE - 1.4.2 (L1) Ensure 'Default Plugin Setting' is set to 'Enabled' (Click to Play) - GPO wording does not match – Ticket #6117
8-15-18	1.3.0	UPDATE - 1.4.2 (L1) Ensure 'Default Plugin Setting' is set to 'Enabled' - Unclear Guidance – Ticket #4766
8-15-18	1.3.0	ADD - 1.1.8.1 (L1) Ensure `Configure native messaging blacklist` is set to 'Enabled' ("*" for all messaging applications) – Ticket #6852
8-15-18	1.3.0	ADD - 1.1.11.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) – Ticket #6853
8-15-18	1.3.0	ADD -1.1.22 (L1) Ensure ‘Enable Site Isolation for every site’ is set to ‘Enabled’ – Ticket #6854
8-15-18	1.3.0	UPDATE – All sections according to the Group Policy Layout using the Newest ADMX templates.